Mend Container

Development to deployment coverage for cloud-native applications.

The Challenge

Cloud-native development brings new potential risks to applications and an added layer of complexity to application security. The customary “shift left” approach finds vulnerabilities in code early during development but misses those vulnerabilities that sneak in later during the containerization process.

Containers put another level of abstraction between security teams and the code, making tracking down vulnerabilities, assessing risk levels, and enforcing policies and other governance difficult. Additional problems, unique to containers, also emerge like poorly stored secrets that can be found by bad actors, potentially handing them the keys to the kingdom.

As with any modern applications, scanning containers can result in a large volume of alerts, many of which are for vulnerabilities that are unreachable at runtime and a typical SCA scan can only give so much insight.

The Mend.io Solution

Using state-of-the-art reachability analysis, Mend Container extends key features of Mend SCA into your container runtime environment and adds entirely new areas of security risk detection and mitigation unique to cloud-native applications.

Mend Container adds key features and benefits to Mend SCA, including:

Container reachability

Mend Container brings the application-level vulnerable method detection customers love in Mend SCA to containers. With Mend Container you can identify which vulnerable files and methods are being called at runtime without the need to install runtime agents.

Secret detection

Mend Container’s secrets detection identifies credentials, passwords, keys, and certificates being exposed or handled inappropriately, putting your applications at risk.

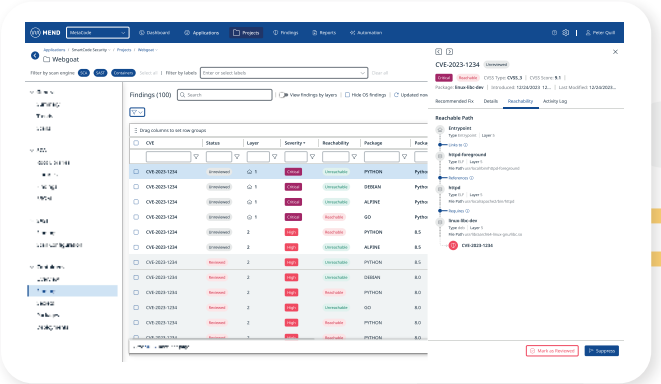
Kubernetes cluster scanning

Effortlessly scan all of your running container images within your Kubernetes clusters, letting you easily find and label containers that are actually in use and deployed.

Development to deployment coverage

Comprehensive container security for your cloud-native applications, starting with static image scans in your pipeline using Mend SCA, all the way to container behavior analysis for security risks in runtime with Mend Container.

Why Mend Container?



Gain a Clear View Across the SDLC.
A comprehensive, dedicated solution for containers, Mend SCA and Mend Container together cover single images to entire registries from development to deployment.

Get Runtime Insights Early. With Mend Container's container-level reachability, you can safely deprioritize more unreachable vulnerabilities than with Mend SCA alone.

Quickly Know What Matters. With runtime monitoring of container images in Kubernetes clusters, organizations can identify which risks are exploitable and require urgent remediation – and which can be safely ignored.

Keep Your Secrets Safe. Find unprotected sensitive information such as API keys and passwords before malicious actors do.

Extend Your SCA Capabilities: The Power of Mend Container

Mend Container integrates with Mend SCA to add robust runtime protection and advanced features beyond software composition analysis.

	Mend SCA	Mend SCA + Mend Container
Enforce Container risk policies	✓	✓
Scan at scale by image registry	✓	✓
Runtime reachability		✓
Kubernetes cluster scanning		✓
Secrets detection		✓

About Mend.io

Trusted by the world's leading companies, including IBM, Google, and Capital One, Mend.io's enterprise suite of application security tools is designed to help you build and manage a mature, proactive AppSec program.

Mend understands the different AppSec requirements of developers and security teams. Unlike other AppSec solutions that force everyone to use a single tool, Mend helps them work in harmony by giving each team different, but complementary, tools—enabling them to stop chasing vulnerabilities and start proactively managing application risk.

Learn more at

Mend.io